Section 3. Storage and Storage Equipment

5-300. General. This Section describes the uniform requirements for the physical protection of classified material in the custody of contractors. Where these requirements are not appropriate for protecting specific types or forms of classified material, compensatory provisions shall be developed and approved by the CSA. Nothing in this Manual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this Manual and at acceptable cost.

5-301. **General Services Administration (GSA) Storage Equipment.** GSA establishes and publishes uniform standards, specifications, and supply schedules for security containers, vault door and frame units, and key-operated and combination padlocks suitable for the storage and protection of classified information. Manufacturers, and prices of storage equipment approved by the GSA, are listed in the Federal Supply Schedule (FSS) catalog (FSC GROUP 7 l-Part HI). Copies of specifications and schedules may be obtained from any regional office of the GSA.

5-302. **TOP SECRET Storage.** TOP SECRET material shall be stored in a GSA-approved security container, an approved vault or an approved Closed Area. Supplemental protection is required.

5-303. **SECRET Storage.** SECRET material shall be stored in the same manner as TOP SECRET material without supplemental protection or as follows:

a. A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours.

b. Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts, so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely, so their contents cannot be removed without forcing open the drawer. This type cabinet will be accorded supplemental protection during non-working hours.

5-304. **CONFIDENTIAL Storage.** CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material except that no supplemental protection is required.

5-305. Restricted **Areas.** When it is necessary to control access to classified material in an open area during working hours, a Restricted Area may be established. A Restricted Area will normally become necessary when it is impractical or impossible to protect classified material because of its size, quantity or other unusual characteristic. The Restricted Area shall have a clearly defined perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority. All classified material will be secured during non-working hours in approved repositories or secured using other methods approved by the CSA.

5-306. **Closed Areas.** Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA and be constructed in accordance with Section 8 of this Chapter. Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a supplanting access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified matenal/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. The Closed Area shall be accorded supplemental protection during non-working hours. During such hours, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, will not require additional locking devices.

a. Open shelf or bin storage of classified documents in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for such approval.

b. The CSA and the contractor shall agree on the need to establish, and the extent of, Closed Areas prior to the award of the contract, when possible, or at such subsequent time as the need for such areas becomes apparent during performance on the contract.

5-307. Supplemental Protection.

a. Intrusion Detection Systems as described in Section 9 of this Chapter shall be used as supplemental protection for all storage containers, vaults and Closed Areas approved for storage of classified material following publication of this Manual.

b. Security guards approved as supplemental protection prior to publication of this Manual may continue to be utilized. When guards are authorized, the schedule of patrol is 2 hours for TOP SECRET material and 4 hours for SECRET material.

c. GSA-approved security containers and approved vaults secured with a locking mechanism meeting Federal Specification FF-L-2740, do not require supplemental protection when the CSA has determined that the GSA-approved security container or approved vault is located in an area of the facility with security-in-depth.

5-308. **Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas. Only a** minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of classified material authorized for storage.

a. A record of the names of persons having knowledge of the combination shall be maintained.

b. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

c. The combination shall be safeguarded in accordance with the highest classification of the material authorized for storage in the container. Superseded combinations shall be destroyed.

d. If a record is made of a combination, the record shall be marked with the highest classification of material authorized for storage in the container.

5-309. **Changing Combinations.** Combinations shall be changed by a person authorized access to the contents of the container, or by the FSO or his or her designee. Combinations shall be changed as follows:

a. The initial use of an approved container or lock for the protection of classified material.

b. The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked.

c. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

d. At other times when considered necessary by the FSO or CSA.

5-310. Supervision of Keys and Padlocks. Use of key-operated padlocks are subject to the following requirements: (i) a key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified material; (ii) a key and lock control register shall be maintained to identify keys for each lock and their current location and custody; (iii) keys and locks shall be audited each month; (iv) keys shall be inventoried with each change of custody; (v) keys shall not be removed from the premises; (vi) keys and spare locks shall be protected equivalent to the level of classified material involved; (vii) locks shall be changed or rotated at least annually, and shall be replaced after loss or compromise of their operable keys; and (viii) making master keys is prohibited.

5-311. Repair of Approved Containers. Repairs, maintenance, or other actions that affect the physical integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers.

a. An approved security container is considered to have been restored to its original state of security integrity if all damaged or altered parts are replaced with manufacturer's replacement or identical cannibalized parts.

b. GSA-approved containers manufactured prior to October 1990, and often referred to as BLACK labeled containers, can be neutralized by drilling a hole adjacent to or through the dial ring of the container, thereby providing access into the locking mechanism to open the lock. Before replacement of the damaged locking mechanism, the drill hole will have to be repaired with a plug which can be: (1) A tapered, hardened tool-steel pin; (2) A steel dowel; (3) A drill bit; or (4) A steel ball bearing. The plug must be of a diameter slightly larger than the hole, and of such length that when driven into the hole there shall remain at each end a shallow recess not less than 1/8 inch or more than 3/ 16 inch deep to permit the acceptance of substantial welds. Additionally, the plug must be welded on both the inside and outside surfaces. The outside of the drawer or door must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains after replacement of the damaged parts with the new lock.

c. GSA-approved containers manufactured after October 1990 and containers equipped with combination locks meeting Federal specification FF-L-2740 require a different method of repair. These containers, sometimes referred to as RED labeled containers, have a substantial increase in lock protection which makes the traditional method of drilling extremely difficult. The process for neutralizing a lockout involves cutting the lock bolts by sawing through the control drawerhead. The only authorized repair is replacement of the drawerhead and locking bolts.

d. Approved security containers that have been drilled or repaired in a manner other than as described above, shall not be considered to have been restored to their original integrity. The "Protection" label on the outside of the locking drawer's side and the "General Services Administration Approved Security Container" label on the face of the top drawer shall be removed.

e. A container repaired using other methods than those described above shall not be used for storage of TOP SECRET material, but may be used for storage of Secret material with the approval of the CSA and for storage of CONFIDENTIAL material with the approval of the FSO.

f. A list shall be maintained by the FSO of all approved

also be on file a signed and dated certification, provided by the repairer, setting forth the method of repair **used.**

5-312. Supplanting Access Control Systems or Devices. Automated access control systems and electronic, mechanical, or electromechanical devices which meet the criteria stated in paragraphs 5-313 and 5-314, below, may be used to supplant contractor-authorized employees or guards to control admittance to Closed and Restricted Areas during working hours. Approval of the FSO is required before effecting the installation of a supplanting access control device to meet a requirement of this Manual.

5-313. **Automated Access Control Systems.** The automated access control system must be capable of identifying the individual entering the area and authenticating that person's authority to enter the area.

a. Manufacturers of automated access control equipment or devices must assure in writing that their system will meet the following standards before FSO'S may favorably consider such systems for protection of classified information:

(1) Chances of an unauthorized individual gaining access through normal operation of the equipment are no more than one in ten thousand.

(2) Chances of an authorized individual being rejected for access through normal operation of the equipment are no more than one in one thousand.

b. Identification of individuals entering the area can be obtained by an identification (ID) badge or card, or by personal identity.

(I) The ID badge or card must use embedded sensors, integrated circuits, magnetic stripes or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal identity verification identifies the individual requesting access by some unique personal characteristic, such as, (a) Fingerprint, (b) Hand geometry, (c) Handwriting, (d) Retina, or (e) Voice recognition.

"

into the system by each individual using a keypad device. The PIN shall consist of four or more digits, randomly selected with no known or logical association with the individual. The PIN must be changed when it is believed to have been subjected to compromise.

d. Authentication of the individual's authorization to enter the area must be accomplished within the system by comparing the inputs from the ID badge or card or the personal identity verification device and the keypad with an electronic database of individuals authorized into the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment. transfer or termination, or when the individual's personnel clearance is suspended or revoked.

e. Locations where access transactions are, or can be displayed, and where authorization data, card **encoded data** and personal identification or verification data is input, stored, displayed, or recorded must be protected.

f. Control panels, card readers, keypads, communication or interface devices located outside the entrance to a Closed Area shall have tamper resistant enclosures, be securely fastened to a wall or other structure, be protected by a tamper alarm or secured with an approved combination padlock. Control panels located within a Closed Area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism. Where areas containing TOP SECRET information are involved, tamper alarm protection is mandatory.

g. **Systems** that utilize transmission lines to carry access authorization, personal identification, or verification data between devices/equipment located outside the Closed Area shall receive circuit protection equal to or greater than that specified as Grade A by UL.

h. Access to records and information concerning encoded ID data and PINs shall be restricted to individuals cleared at the same level as the highest classified information contained within the specific area or areas in which ID data or PLNs are utilized. Access to identification or authorization data, operating system software or any identifying data associated with the access control system shall be limited to the least number of personnel possible. Such data or software shall be kept secured when unattended.

i. Records reflecting active assignments of ID badges/cards, PINs, levels of access, personnel clearances, and similar system related records shall be maintained. Records concerning personnel removed from the system shall be retained for 90 days.

j. Personnel entering or leaving an area shall be required to immediately secure the entrance or exit point. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's clearance and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor-authorized employee or guard stationed to supervise the entrance to the area.

5-314. **Electronic, Mechanical, or Electro-mechanical Devices.** Provided the classified material within the Closed Area is no "higher than SECRET, electronic, mechanical, or electro-mechanical devices that meet the criteria stated in this paragraph may be used to supplant contractor authorized employees or guards to control admittance to Closed Areas during working hours. Devices may be used that operate by either a push-button combination that activates the locking device or by a control card used in conjunction with a push-button combination, thereby excluding any system that operates solely by the use of a control card.

a. The electronic control panel containing the mechanical mechanism by which the combination is set may be located inside or outside the Closed Area. When located outside the Closed Area, the control panel shall be securely fastened or attached to the perimeter barrier of the area and secured by an approved combination padlock. If the control panel is located within the Closed Area, it shall require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.

b. The control panel shall be installed in a manner that precludes an unauthorized person in the immediate vicinity from observing the selection of the correct combination of the push buttons, or have a shielding device mounted.

c. The selection and setting of the combination shall be accomplished by an employee of the contractor who is authorized to enter the area. The combination shall be changed as specified in paragraph 5-309. The combination shall be classified and safeguarded in accordance with the classification of the highest classified material within the Closed Area.

d. Electrical gear, wiring included, or mechanical links (cables, rods, etc.) shall be accessible only from inside the area, or shall be secured within a protective covering to preclude surreptitious manipulation of components.

e. Personnel entering or leaving the area shall be required to immediately lock the entrance or exit point. Authorized personnel *who permit another* individual entrance into the area are responsible for confirming the individual's personnel clearance and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor authorized employee or guard stationed to supervise the entrance to the area.